

DEVICE AND METHOD FOR GENERATING CRYPTOGRAPHIC KEY, DEVICE AND METHOD FOR ENCIPHERING AND DECIPHERING, AND PROGRAM PROVIDING MEDIUM

Publication number: JP2001144748 (A)

Publication date: 2001-05-25

Inventor(s): MIZUTANI YOICHI; WATANABE KOICHIRO

Applicant(s): SONY CORP

Classification:

- international: **H04L9/32; H04L9/32; (IPC1-7): H04L9/32**

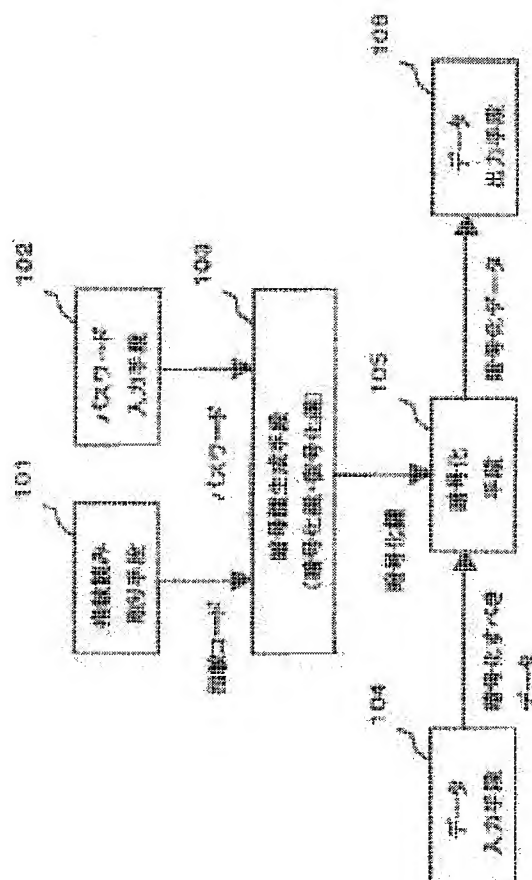
- European:

Application number: JP19990320895 19991111

Priority number(s): JP19990320895 19991111

Abstract of JP 2001144748 (A)

PROBLEM TO BE SOLVED: To provide a cryptographic key generating device and an encoding and decoding device which eliminate the necessity of registering user's bionic information and whose security management is easy. **SOLUTION:** A cryptographic key is generated on the basis of not only the bionic information but a synthetic code obtained by combining an optional password with the bionic information. An intermediate code is generated on the basis of a code acquired by reading the bionic information such as a fingerprint pattern and the password inputted by the user, the cryptographic key such as an encryption key and a decryption key is generated on the basis of the generated intermediate code, and enciphering and deciphering are carried out. Meanwhile, the user's bionic information does not have to be preliminarily registered in a storage device, etc., and it is further possible to generate an infinite number of different encryption or decryption keys by changing passwords.



Data supplied from the **esp@cenet** database — Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-144748
(P2001-144748A)

(43) 公開日 平成13年5月25日 (2001.5.25)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 L	9/32	H 0 4 L 9/00	6 7 3 D 5 J 1 0 4 6 7 3 A

審査請求 未請求 請求項の数24 O L (全 16 頁)

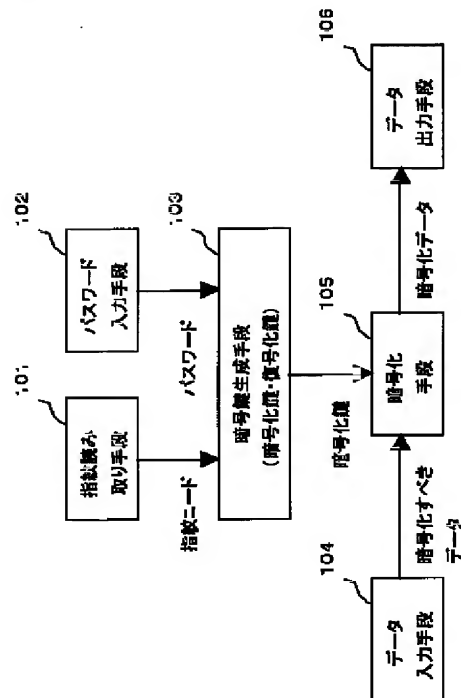
(21) 出願番号	特願平11-320895	(71) 出願人	000002185 ソニー株式会社 東京都品川区北品川6丁目7番35号
(22) 出願日	平成11年11月11日 (1999. 11. 11)	(72) 発明者	水谷 陽一 東京都品川区北品川6丁目7番35号 ソニー株式会社内
		(72) 発明者	渡邊 浩一郎 東京都品川区北品川6丁目7番35号 ソニー株式会社内
		(74) 代理人	100101801 弁理士 山田 英治 (外2名) Fターム(参考) 5J104 AA07 AA27 AA41 EA08 EA25 KA01 KA17 KA19 NA02 NA05 NA30 PA10 PA12 PA14

(54) 【発明の名称】 暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法、並びにプログラム提供媒体

(57) 【要約】

【課題】 ユーザの生体情報を登録する必要性を排除し、セキュリティ管理の容易な暗号鍵生成装置、暗号化・復号化装置を提供する。

【解決手段】 生体情報のみではなく、任意のパスワードを生体情報に組み合わせた合成コードに基づいて暗号鍵を生成する構成とした。指紋パターン等の生体情報の読み取りによって取得するコードとユーザの入力するパスワードに基づいて中間コードを生成して、生成した中間コードに基づいて暗号化鍵、復号化鍵等の暗号鍵を生成し、暗号化・復号化を実行する。生成された鍵はユーザ固有のものであることが保証され、一方、記憶装置等に予めユーザの生体情報を登録する必要がなく、さらにパスワードの変更により無限数の異なる暗号化鍵または復号化鍵の生成が可能となる。



【特許請求の範囲】

【請求項1】生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、パスワードを入力するパスワード入力手段と、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに基づいて中間コードを生成する中間コード生成手段と、前記中間コードに基づいて、暗号化処理または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、を有することを特徴とする暗号鍵生成装置。

【請求項2】前記生体情報読み取り手段の読み取る生体情報は、指紋、眼底像、声紋、DNAパターンのいずれか、または指紋、眼底像、声紋、DNAパターンの2以上の生体情報の組み合わせであることを特徴とする請求項1に記載の暗号鍵生成装置。

【請求項3】前記生体情報読み取り手段の読み取る生体情報は指紋情報であり、前記生体情報読み取り手段は、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力する構成であることを特徴とする請求項1に記載の暗号鍵生成装置。

【請求項4】前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードとのいずれか一方を上位ビットとし、他方を下位ビットとする生体コードおよびパスワードのデータ接続処理を実行して中間コードを生成する構成であることを特徴とする請求項1に記載の暗号鍵生成装置。

【請求項5】前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに対して関数を適用して新たな中間コードを生成する構成であることを特徴とする請求項1に記載の暗号鍵生成装置。

【請求項6】前記暗号鍵生成手段の生成する暗号鍵は、共通鍵暗号化方式における共通鍵、公開鍵暗号化方式における公開鍵、秘密鍵のいずれかであることを特徴とする請求項1に記載の暗号鍵生成装置。

【請求項7】生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、パスワードを入力するパスワード入力手段と、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに基づいて中間コードを生成する中間コード生成手段と、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、暗号化すべきデータを入力するデータ入力手段と、

前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力手段から入力したデータの暗号化処理を実行する暗号化手段と、

前記暗号化手段において暗号化したデータを出力する出力手段と、を有することを特徴とする暗号化装置。

【請求項8】前記生体情報読み取り手段の読み取る生体情報は、指紋、眼底像、声紋、DNAパターンのいずれか、または指紋、眼底像、声紋、DNAパターンの2以上の生体情報の組み合わせであることを特徴とする請求項7に記載の暗号化装置。

【請求項9】前記生体情報読み取り手段の読み取る前記生体情報は指紋情報であり、前記生体情報読み取り手段は、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力する構成であることを特徴とする請求項7に記載の暗号化装置。

【請求項10】前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードとのいずれか一方を上位ビットとし、他方を下位ビットとする生体コードおよびパスワードのデータ接続処理を実行して中間コードを生成する構成であることを特徴とする請求項7に記載の暗号化装置。

【請求項11】前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに対して関数を適用して新たな中間コードを生成する構成であることを特徴とする請求項7に記載の暗号化装置。

【請求項12】生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、

パスワードを入力するパスワード入力手段と、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに基づいて中間コードを生成する中間コード生成手段と、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、復号化すべきデータを入力するデータ入力手段と、前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力手段から入力したデータの復号化処理を実行する復号化手段と、前記復号化手段において復号化したデータを出力する出力手段と、を有することを特徴とする復号化装置。

【請求項13】前記生体情報読み取り手段の読み取る生体情報は、指紋、眼底像、声紋、DNAパターンのいずれか、または指紋、眼底像、声紋、DNAパターンの2

以上の生体情報の組み合わせであることを特徴とする請求項12に記載の復号化装置。

【請求項14】前記生体情報読み取り手段の読み取る前記生体情報は指紋情報であり、前記生体情報読み取り手段は、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力する構成であることを特徴とする請求項12に記載の復号化装置。

【請求項15】前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードとのいずれか一方を上位ビットとし、他方を下位ビットとする生体コードおよびパスワードのデータ接続処理を実行して中間コードを生成する構成であることを特徴とする請求項12に記載の復号化装置。

【請求項16】前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに対して関数を適用して新たな中間コードを生成する構成であることを特徴とする請求項12に記載の復号化装置。

【請求項17】暗号化処理または復号化処理に使用する暗号鍵を生成する暗号鍵生成方法において、生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、パスワードを入力するパスワード入力ステップと、前記生体情報読み取りステップにおいて読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードに基づいて中間コードを生成する中間コード生成ステップと、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、を有することを特徴とする暗号鍵生成方法。

【請求項18】前記生体情報読み取りステップにおいて読み取る生体情報は、指紋、眼底像、声紋、DNAパターンのいずれか、または指紋、眼底像、声紋、DNAパターンの2以上の生体情報の組み合わせであることを特徴とする請求項17に記載の暗号鍵生成方法。

【請求項19】前記生体情報読み取りステップにおいて読み取る前記生体情報は指紋情報であり、前記生体情報読み取りステップは、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力することを特徴とする請求項17に記載の暗号鍵生成方法。

【請求項20】前記中間コード生成ステップは、前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップで入力されたパスワードとの

いずれか一方を上位ビットとし、他方を下位ビットとする生体コードおよびパスワードのデータ接続処理を実行して中間コードを生成するステップを含むことを特徴とする請求項17に記載の暗号鍵生成方法。

【請求項21】前記中間コード生成ステップは、前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップで入力されたパスワードに対して関数を適用して新たな中間コードを生成するステップを含むことを特徴とする請求項17に記載の暗号鍵生成方法。

【請求項22】生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、パスワードを入力するパスワード入力ステップと、前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードに基づいて中間コードを生成する中間コード生成ステップと、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、暗号化すべきデータを入力するデータ入力ステップと、前記暗号鍵生成ステップにおいて生成した暗号鍵に基づいて前記データ入力ステップにおいて入力したデータの暗号化処理を実行する暗号化ステップと、前記暗号化ステップにおいて暗号化したデータを出力する出力ステップと、を有することを特徴とする暗号化方法。

【請求項23】生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、パスワードを入力するパスワード入力ステップと、前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップで入力されたパスワードに基づいて中間コードを生成する中間コード生成ステップと、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、復号化すべきデータを入力するデータ入力ステップと、前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力ステップにおいて入力したデータの復号化処理を実行する復号化ステップと、前記復号化ステップにおいて復号化したデータを出力する出力ステップと、を有することを特徴とする復号化方法。

【請求項24】暗号鍵生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを有形的に提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、パスワードを入力するパスワード入力ステップと、前記生体情報読み取りステップにおいて読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードに基づいて中間コードを生成する中間コード生成ステップと、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術的分野】本発明は、暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法、並びにプログラム提供媒体に関する。さらに詳細には、指紋等、個人固有の生体情報とパスワードとを組み合わせたデータに基づいて暗号化鍵、復号化鍵を生成する暗号鍵生成装置および方法に関するものであり、さらに、機密保持の要請される文書データ、音声データ、画像データ、各種プログラム等、様々な情報の暗号化処理、復号化処理を生体情報とパスワードとを組み合わせたデータに基づく暗号化鍵、復号化鍵を用いて行なう暗号化・復号化装置および暗号化・復号化方法に関するものである。

【0002】

【従来の技術】近年、インターネット等の各種ネットワークシステムを介した情報転送が盛んになり、ネットワーク上での電子決済や電子マネーの使用が急激に増大している。さらに多くの企業、あるいは個人において機密文書をハードディスク、光ディスク等、様々な記憶媒体を利用して保存することも頻繁に行われている。このようなネットワークを介する転送データ、あるいは様々な記憶媒体に格納されるデータのセキュリティをいかに確保するかが重要な課題となっている。

【0003】セキュリティ確保の方法には様々な手法があるが、その一つがコンピュータの利用を正規の利用者に限定する方法である。この方法の代表的なものは、予め正規利用者に対してパスワードを与え、正しいパスワードの入力を行なった者のみがデータへのアクセスを可能とする構成である。さらに、セキュリティを高めるためのデータ自体に対する処理としてデータの暗号化処理がある。ネットワークを介して転送する文書を暗号化し、また、記憶媒体に格納する情報を暗号化処理することにより、転送情報および蓄積情報の安全性を高めることができる。

【0004】暗号化データは、所定の手続きによる復号化によって解読可能な文書（平文）に戻すことができる。情報の暗号化処理に暗号化鍵を用い、復号化に復号化鍵を用いるデータ暗号化、復号化方法が従来から知ら

れている。

【0005】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その1つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にDES（データ暗号標準：Data encryption standard）がある。

【0006】また、暗号化するとき使用する暗号化鍵による処理と、復号するとき使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはRSA（Rivest-Shamir-Adleman）暗号がある。

【0007】前述の共通鍵暗号化方式は、想定される通信相手数が多くなると鍵の数が膨大となり、不特定多数の通信には向かない。また、公開鍵暗号化方式は、管理する鍵の数は少なくすむという利点がある。しかし、公開鍵暗号化方式は暗号化処理、復号化が煩雑になるという欠点がある。

【0008】上述の共通鍵暗号化方式と、公開鍵暗号化方式とを融合させた方式としてハイブリッド暗号化方式がある。ハイブリッド暗号化方式は、情報の暗号化には共通鍵を用い、暗号化に用いた共通鍵を公開鍵暗号化方式で暗号化するものである。このハイブリッド暗号化方式によれば、処理の早い共通鍵暗号化方式をデータ量の多い文書に適用し、処理の遅い公開鍵暗号化方式をデータ量の少ない共通鍵の暗号化にのみ使用するので、両者の利点を有効に利用できる。

【0009】上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザID等のパスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるユーザID等のパスワードを求めることは実質上不可能である。

【0010】上述の観点から、暗号化鍵、復号化鍵を用いる構成においては、パスワード管理がセキュリティ管理上、非常に重要な問題となる。しかしながら、ユーザID等のパスワードを個人で管理することには様々な問題があるのが現状である。セキュリティを高めるためには複雑なパスワードを持つことが有利と考えられるが、複雑なパスワードを人間が記憶することは困難である。人間の記憶を補うために例えばハードディスク等何らかの記憶装置にパスワードを記憶させて保存することも可能であるが、このような記憶装置にパスワードを格納した場合、第三者が記憶装置からパスワードを盗むという可能性もあり、安全性に関して問題がある。

【0011】パスワード管理の問題点を解決するための一つの手法として、個人の生体情報、例えば眼底像、指紋等を用いて、正規ユーザであるか否かの照合を行なう方法がある。個人の生体情報を用いたセキュリティ管理システム例として、特開平11-215119号公報に開示の個人情報管理装置および方法がある。

【0012】特開平11-215119号公報に記載のシステムは、正規ユーザ個人の生体情報、例えば眼底像から得られるコード情報を予めシステムに登録して保存する構成を持つ。本システムは、文書の暗号化処理を行なおうとするユーザが、まず自分の眼底情報等、生体情報の読み取りをシステムに実行させる。次に、システムは、ユーザが正規の登録済みユーザであるか否かについて、ユーザから読み取った生体情報と登録した生体情報とを比較照合して確認する。この照合処理によってユーザの正当性が確認された場合にのみ、生体情報に基づく鍵によって暗号化処理に移行する構成としたものである。この方法によれば、個人固有の生体情報に基づく秘密鍵を用いて暗号化処理が実行されるので、他人による秘密鍵の複製、悪用が防止されるという効果がある。

【0013】

【発明が解決しようとする課題】しかしながら、このような生体情報を用いた個人の正当性確認処理を実現するためには、新たに読み取った個人の眼底像、指紋等の生体情報と比較対象となる照合情報をシステム中の記憶装置中に格納しておく必要がある。すなわち正規ユーザである各個人の眼底像、指紋等を予め電子撮影して得られた画像情報、あるいは、この画像情報から得られるコード列を予め記憶装置に記憶することが必要となる。特開平11-215119号では生体情報から得られるコードを変換処理した2次コードを保存することにより安全性を高めているが、このようなシステムでは、記憶情報が盗用されてしまった場合に、盗用された情報に基づいて暗号鍵が複製される可能性があり、システムの信頼性が必ずしも十分ではない。

【0014】さらに、従来の生体情報のみに頼るコード生成手法では、異なる個人の指紋等から読み取られる生体情報コードが同一になってしまうと、その同一コード

に基づいて同一の暗号鍵が生成される可能性がある。このような可能性を排除するため、スキャナ等の生体情報読み取り手段のパターン読み取り精度を極めて高精度にして各個人の生体情報コードを確実に異なるものとしなければならなかった。しかし、現実には、そのような高精度な読み取りを実現させることは困難であり、また高精度な読み取りを実現させようすると、たとえ同一人であっても読み取り毎に異なるコードが生成されるなどの不具合が発生する可能性があり、現実として使用に耐えるシステムを実現するのは困難である。

【0015】さらに、従来のシステム構成では、正規ユーザの眼底像等、生体情報を予め電子撮影した画像情報、あるいは、それらの画像情報から得られるコード列を記憶した記憶装置を持たないシステムにおいては照合処理が不可能である。従って、ネットワークを介した暗号情報配信システム等上記構成を適用した場合は、照合情報を蓄積したメモリを搭載した装置のみが通信に参加することができ、照合情報を蓄積していない装置は通信に参加できないことになる。従って、上記構成は極めて限定されたシステムにおいてのみ有効な構成であって拡張性に劣るという欠点がある。

【0016】さらに、特開平11-215119号公報に開示の個人情報管理装置および方法のように、眼底像情報に基づいて暗号化鍵を生成しようとする場合、個人から得られる眼底像情報は、左右の目を使用した場合でも2つであり、眼底像情報から得られるコード列は極めて少ない種類となるので暗号化鍵の種類を増やすことは困難となる。さらに異なる暗号鍵を作成しようとした場合、他の生体情報、例えば指紋を使用することが考えられるが10本の指を使用した場合でも、最大10種類のコードが得られるのみであるので、生体情報のみを使用した暗号化鍵生成方法において生成される暗号鍵は極めて限定された有限数に限られてしまうという問題がある。

【0017】本発明の、暗号化・復号化装置および暗号化・復号化方法、並びにプログラム提供媒体は、上述のような従来技術における問題点に鑑みてなされたものである。

【0018】本発明は、生体情報のみではなく、任意のパスワードを生体情報に組み合わせた合成コードに基づいて暗号鍵を生成する構成とすることにより、異なる個人において生体情報が万が一、一致した場合であっても、パスワードとの組み合わせで生成されるコードの一致する可能性をなくし、指紋パターン等の生体情報の読み取りによって取得するコードを極めて簡単な構成とすることを可能とした暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法を提供することを目的とする。

【0019】さらに、本発明の、暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化

方法は、生体情報を用いた暗号化鍵または復号化鍵生成手法を用いたシステムは、記憶装置等に予め正規ユーザの生体情報を登録する必要性を排除してシステムの拡張性を確保したシステムを提供することを目的とする。

【0020】さらに、本発明は、生体情報にパスワードを組み合わせたコード列に基づいて暗号化鍵、または復号化鍵を生成する構成とすることにより、無限数の異なる暗号化鍵または復号化鍵の生成を可能とした暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法を提供することを目的とする。

【0021】

【課題を解決するための手段】本発明の第1の側面は、生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、パスワードを入力するパスワード入力手段と、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに基づいて中間コードを生成する中間コード生成手段と、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、を有することを特徴とする暗号鍵生成装置にある。

【0022】さらに、本発明の暗号鍵生成装置において、前記生体情報読み取り手段の読み取る生体情報は、指紋、眼底像、声紋、DNAパターンのいずれか、または指紋、眼底像、声紋、DNAパターンの2以上の生体情報の組み合わせであることを特徴とする。

【0023】さらに、本発明の暗号鍵生成装置において、前記生体情報読み取り手段の読み取る生体情報は指紋情報であり、前記生体情報読み取り手段は、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力する構成であることを特徴とする。

【0024】さらに、本発明の暗号鍵生成装置において、前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードとのいずれか一方を上位ビットとし、他方を下位ビットとする生体コードおよびパスワードのデータ連接処理を実行して中間コードを生成する構成であることを特徴とする。

【0025】さらに、本発明の暗号鍵生成装置において、前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに対して関数を適用して新たな中間コードを生成する構成であることを特徴とする。

【0026】さらに、本発明の暗号鍵生成装置において、前記暗号鍵生成手段の生成する暗号鍵は、共通鍵暗号化方式における共通鍵、公開鍵暗号化方式における公開鍵、秘密鍵のいずれかであることを特徴とする。

【0027】さらに、本発明の第2の側面は、生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、パスワードを入力するパスワード入力手段と、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに基づいて中間コードを生成する中間コード生成手段と、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、暗号化すべきデータを入力するデータ入力手段と、前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力手段から入力したデータの暗号化処理を実行する暗号化手段と、前記暗号化手段において暗号化したデータを出力する出力手段と、を有することを特徴とする暗号化装置にある。

【0028】さらに、本発明の暗号化装置において、生体情報読み取り手段の読み取る生体情報は、指紋、眼底像、声紋、DNAパターンのいずれか、または指紋、眼底像、声紋、DNAパターンの2以上の生体情報の組み合わせであることを特徴とする。

【0029】さらに、本発明の暗号化装置において、前記生体情報読み取り手段の読み取る前記生体情報は指紋情報であり、前記生体情報読み取り手段は、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力する構成であることを特徴とする。

【0030】さらに、本発明の暗号化装置において、前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードとのいずれか一方を上位ビットとし、他方を下位ビットとする生体コードおよびパスワードのデータ連接処理を実行して中間コードを生成する構成であることを特徴とする。

【0031】さらに、本発明の暗号化装置において、前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに対して関数を適用して新たな中間コードを生成する構成であることを特徴とする。

【0032】さらに、本発明の第3の側面は、生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取り手段と、パスワードを入力するパスワード入力手段と、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに基づいて中間コードを生成する中間コード生成手段と、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成手段と、復号化すべきデータを入力するデータ入力手段と、前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力手段から入力し

たデータの復号化処理を実行する復号化手段と、前記復号化手段において復号化したデータを出力する出力手段と、を有することを特徴とする復号化装置にある。

【0033】さらに、本発明の復号化装置において、生体情報読み取り手段の読み取る生体情報は、指紋、眼底像、声紋、DNAパターンのいずれか、または指紋、眼底像、声紋、DNAパターンの2以上の生体情報の組み合わせであることを特徴とする。

【0034】さらに、本発明の復号化装置において、前記生体情報読み取り手段の読み取る前記生体情報は指紋情報であり、前記生体情報読み取り手段は、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力する構成であることを特徴とする。

【0035】さらに、本発明の復号化装置において、前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードとのいずれか一方を上位ビットとし、他方を下位ビットとする生体コードおよびパスワードのデータ接続処理を実行して中間コードを生成する構成であることを特徴とする。

【0036】さらに、本発明の復号化装置において、前記中間コード生成手段は、前記生体情報読み取り手段で読み取られ生成された生体コードと上記パスワード入力手段から入力されたパスワードに対して関数を適用して新たな中間コードを生成する構成であることを特徴とする。

【0037】さらに、本発明の第4の側面は、暗号化処理または復号化処理に使用する暗号鍵を生成する暗号鍵生成方法において、生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、パスワードを入力するパスワード入力ステップと、前記生体情報読み取りステップにおいて読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードに基づいて中間コードを生成する中間コード生成ステップと、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、を有することを特徴とする暗号鍵生成方法にある。

【0038】さらに、本発明の暗号鍵生成方法において、生体情報読み取りステップにおいて読み取る生体情報は、指紋、眼底像、声紋、DNAパターンのいずれか、または指紋、眼底像、声紋、DNAパターンの2以上の生体情報の組み合わせであることを特徴とする。

【0039】さらに、本発明の暗号鍵生成方法において、前記生体情報読み取りステップにおいて読み取る前記生体情報は指紋情報であり、前記生体情報読み取りステップは、指紋画像を分割した複数領域において指紋の凹凸パターンの形成する隆線方向を識別し、該隆線方向

に応じたコードを前記複数領域毎に対応付けることにより生体コードを生成して出力することを特徴とする。

【0040】さらに、本発明の暗号鍵生成方法において、前記中間コード生成ステップは、前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップで入力されたパスワードとのいずれか一方を上位ビットとし、他方を下位ビットとする生体コードおよびパスワードのデータ接続処理を実行して中間コードを生成するステップを含むことを特徴とする。

【0041】さらに、本発明の暗号鍵生成方法において、前記中間コード生成ステップは、前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップで入力されたパスワードに対して関数を適用して新たな中間コードを生成するステップを含むことを特徴とする。

【0042】さらに、本発明の第5の側面は、生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、パスワードを入力するパスワード入力ステップと、前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードに基づいて中間コードを生成する中間コード生成ステップと、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、暗号化すべきデータを入力するデータ入力ステップと、前記暗号鍵生成ステップにおいて生成した暗号鍵に基づいて前記データ入力ステップにおいて入力したデータの暗号化処理を実行する暗号化ステップと、前記暗号化ステップにおいて暗号化したデータを出力する出力ステップと、を有することを特徴とする暗号化方法にある。

【0043】さらに、本発明の第6の側面は、生体情報を取得し、該生体情報に基づく生体コードを生成して出力する生体情報読み取りステップと、パスワードを入力するパスワード入力ステップと、前記生体情報読み取りステップで読み取られた生体コードと上記パスワード入力ステップで入力されたパスワードに基づいて中間コードを生成する中間コード生成ステップと、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、復号化すべきデータを入力するデータ入力ステップと、前記暗号鍵生成手段において生成した暗号鍵に基づいて前記データ入力ステップにおいて入力したデータの復号化処理を実行する復号化ステップと、前記復号化ステップにおいて復号化したデータを出力する出力ステップと、を有することを特徴とする復号化方法にある。

【0044】さらに、本発明の第7の側面は、暗号鍵生成処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを有形的に提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、生体情報を取得し、該生体情報に基づく生体コードを生成

して出力する生体情報読み取りステップと、パスワードを入力するパスワード入力ステップと、前記生体情報読み取りステップにおいて読み取られた生体コードと上記パスワード入力ステップにおいて入力されたパスワードに基づいて中間コードを生成する中間コード生成ステップと、前記中間コードに基づいて、暗号化処理、または復号化処理に適用する暗号鍵を生成する暗号鍵生成ステップと、を有することを特徴とするプログラム提供媒体にある。

【0045】本発明の第7の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0046】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0047】

【作用】本発明の構成によれば、指紋コードのような各種の生体情報とパスワードとを組み合わせた合成コードを生成し、この合成コードに基づいて暗号鍵を生成する構成であるので、パスワードによる合成コードのユニーク性を高めることが可能となり、異なる個人間において読み取り生体情報が万が一、一致した場合であっても、パスワードとの組み合わせで生成されるコードは異なるものとすることが可能となり、指紋パターン等の生体情報の読み取りによって取得するコードを極めて簡単なコードとすることが可能となり、高精度の読み取り装置を必要としない暗号化・復号化装置構成が実現される。

【0048】また、本発明の構成によれば、パスワードのみからは同じ暗号鍵を生成することができないので、記憶装置にパスワードを記憶して管理することができ、従って暗号鍵の生成および機密管理が容易となる。ここで、共有の暗号鍵（共有鍵）とは、ユーザ間で共有したい鍵をいい、鍵自体は共通鍵、公開鍵を問わない。すなわち、DES暗号などの共通鍵方式のときは共通鍵を、RSA暗号などの公開鍵方式のときは秘密鍵（秘密の復号化鍵、認証の場合には、秘密の通信文検査鍵）を意味する。なお、公開鍵方式において、暗号化鍵、通信文生成鍵は公開ファイルによってすでに共有されているといえる。

【0049】本発明のさらに他の目的、特徴や利点は、

後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0050】

【発明の実施の形態】以下、本発明の暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法の実施の形態について、図面を参照しながら、詳細に説明する。

【0051】

【実施例】図1に本発明の暗号化装置、図2に復号化装置、図3に暗号化／復号化装置の各構成を示すブロック図を示す。さらに、図4に各構成におけるハードウェア構成例を示す。以下、各図に従って、順次説明する。

【0052】図1は、本発明の暗号化・復号化装置の一実施例に係る暗号化装置を構成するブロック図を示したものである。

【0053】暗号化装置は図1に示すように、指紋読み取り手段101、パスワード入力手段102、暗号鍵生成手段103、データ入力手段104、暗号化手段105、データ出力手段106を有する。なお、以下の実施例の説明においては、図1の暗号化装置に示すように、生体情報として指紋を使用する例を中心として説明する。しかしながら、本発明の暗号化・復号化装置および暗号化・復号化方法で使用する生体情報は、指紋に限らず、眼底像、声紋、DNAパターン、その他、個人特有の生体に関する情報、あるいはこれらの組み合わせであれば使用可能であり、実施例に示す構成に限定されない。眼底像、声紋、DNAパターンを使用する場合は、それぞれの生体情報に対する読み取り装置、分析装置を使用する。例えば眼底像をしようする場合は眼底カメラ、声紋を使用する場合は音声認識装置、DNAパターンを使用する場合はDNA分析装置等を用いて生体情報を読み取る。ただし、以下では、説明の複雑化をさけるため、生体情報として指紋を使用した例について説明する。

【0054】図1の暗号化装置における指紋読み取り手段101は、利用者（ユーザ）の指が押し当てられたときに、指紋パターンを読み取り、その特徴抽出を行い、抽出された特徴データに基づいて指紋コードを出力し、暗号鍵生成手段103に出力する。指紋パターンの読み取りは光学的に指紋を読み取るスキャナ、あるいは指を押し当てることによって発生する圧力を微小部分毎に検出して凹凸パターンを読み取る圧力センサ等、各種の読み取り構成によって実現可能である。

【0055】パスワード入力手段102は、例えばキーボードのようなユーザがパスワードを入力する手段である。パスワード入力手段102から入力されたパスワードは暗号鍵生成手段103に出力される。

【0056】暗号鍵生成手段103は、指紋読み取り手段101から読み取られた指紋コードとパスワード入力手段102から入力されたパスワードの組み合わせに依

じて、暗号鍵を生成し、暗号化手段105へ出力する。この暗号鍵生成手段103で生成する暗号鍵には、暗号化するための暗号化鍵と、復号化するための復号化鍵を含むものであり、前述した共通鍵暗号化方式、公開鍵暗号化方式、ハイブリッド暗号化方式等、各種の暗号化方式のいずれを適用するかによって、生成する鍵の種類が決定されることになる。本発明は、いずれの暗号化方式においても適用可能なものであり、生成する鍵は、データの暗号化処理または復号化処理、あるいは前述のハイブリッド方式を適用する場合には、鍵自体の暗号化処理または復号化処理においても用いられる。この図1では、データの暗号化処理に用いる暗号化鍵を生成したもののとして、以下説明する。なお、暗号鍵生成手段の具体例については、後段で説明する。

【0057】データ入力手段104は、暗号化すべきデータをを入力するたとえばハードディスク、ネットワークインタフェース等によって構成されるデータ入力手段であり、暗号化すべきデータを暗号化手段105へ出力する。暗号化手段105は、データ入力手段104から入力された暗号化すべきデータを、暗号鍵生成手段103で生成された暗号化鍵で暗号化し、データ出力手段106へ出力する。

【0058】データ出力手段106は、ネットワークインタフェース、あるいはハードディスク等の記憶手段等によって構成され、暗号化手段105で暗号化されたデータを出力する。

【0059】図1に示す暗号化装置では、指紋読み取り手段101において指紋から取得される特徴コードと、パスワード入力手段102から入力されるパスワードの組み合わせに応じて、暗号鍵生成手段103が暗号化鍵を生成し、この暗号化鍵により、データ入力手段104から入力したデータを暗号化してデータ出力手段106に出力することが可能であり、指紋読み取り手段101によって読み取られる生体情報に基づくコードが一律のデータであっても、そのコード列にパスワード入力手段102から入力する任意のパスワードを組み合わせると暗号化鍵生成用コードとすることができるので、パスワードを変更することにより無数の異なるコード列を生成することができ、異なる暗号化鍵を無限に生成することが可能となる。

【0060】さらに、図1に示す暗号化装置では、指紋読み取りデータを照合するための照合データを記憶手段に記憶することがないので、第三者による照合データの盗難の恐れがなく、不正に暗号鍵を複製される恐れがない。

【0061】次に、図2を用いて本発明による復号化装置の構成を説明する。図2は、本発明に係る復号化装置の構成を示したブロック図である。図2に示すように復号化装置は、指紋読み取り手段201、パスワード入力手段202、暗号鍵生成手段203、データ入力手段2

04、復号化手段205、データ出力手段206を有する。

【0062】指紋読み取り手段201、パスワード入力手段202、暗号鍵生成手段203、データ入力手段204、データ出力手段206の基本構成は、前述の図1で説明した暗号化装置における各手段と同様であるので、同一構成についての説明は省略し、異なる部分を中心として説明する。

【0063】図2に示す復号化装置において、暗号鍵生成手段203は、指紋読み取り手段201から読み取られた指紋コードとパスワード入力手段202から入力されたパスワードの組み合わせに応じて、暗号鍵、この場合は暗号データの復号化に用いる復号化鍵を生成し、復号化手段205へ出力する。

【0064】データ入力手段204は、復号化すべき暗号化データを入力し、復号化手段205へ出力する。復号化手段205は、データ入力手段204から入力された復号化すべき暗号データを、暗号鍵生成手段203で生成された復号化鍵で復号し、データ出力手段206へ出力する。データ出力手段206は、復号化手段205で、復号化されたデータを出力する。

【0065】この図2に示す復号化装置を用いれば、指紋から取得される特徴コードとパスワードの組み合わせに応じて生成される復号化鍵により、暗号データを復号化して出力することが可能であり、指紋読み取り手段によって読み取られる生体情報に基づくコードが一律のデータであっても、そのコード列に任意のパスワードを組み合わせると復号化鍵の元データとすることができ、パスワードを変更することにより無数の異なるコード列を生成することができるので、異なる無数の復号化鍵を生成することが可能となる。

【0066】また、指紋読み取りデータを照合するための照合データを記憶手段に記憶することがないので、第三者による照合データの盗難の恐れがなく、不正に暗号鍵を複製される恐れがない。

【0067】次に、図3を用いて本発明による暗号化・復号化装置の構成を説明する。図3は、本発明による暗号化・復号化装置の構成を示したブロック図である。図3に示すように暗号化・復号化装置は、指紋読み取り手段301、パスワード入力手段302、暗号鍵生成手段303、データ入力手段304、暗号化・復号化手段305、データ出力手段306を有する。

【0068】指紋読み取り手段301、パスワード入力手段302、暗号鍵生成手段303、データ入力手段304、データ出力手段306の基本構成は、前述の図1、2で説明した暗号化装置、復号化装置における各手段と同様であるので、同一構成についての説明は省略し、異なる部分を中心として説明する。

【0069】図3に示す暗号化・復号化装置において、暗号鍵生成手段303は、指紋読み取り手段301から

読み取られた指紋コードとパスワード入力手段302から入力されたパスワードの組み合わせに応じて、暗号鍵、この場合はデータの暗号化に用いる暗号化鍵、または暗号データの復号化に用いる復号化鍵を生成し、暗号化・復号化手段305へ出力する。

【0070】データ入力手段304は、暗号化すべきデータ、または復号化すべき暗号化データを入力し、暗号化・復号化手段305へ出力する。暗号化・復号化手段305は、データ入力手段304から入力された暗号化すべきデータ、または復号化すべき暗号データを、暗号鍵生成手段303で生成された暗号化鍵で暗号化処理、または復号化鍵で復号し、データ出力手段306へ出力する。データ出力手段306は、暗号化手段305で暗号化されたデータ、または、復号されたデータを出力する。

【0071】この図3に示す暗号化・復号化装置においても、前述の暗号化装置、または復号化装置と同様に、指紋から取得される特徴コードとパスワードの組み合わせに応じて生成される暗号化鍵、または復号化鍵により、データの暗号化処理または復号化が可能となり、指紋読み取り手段によって読み取られる生体情報に基づくコードが一律のデータであっても、そのコード列に任意のパスワードを組み合わせる暗号化鍵、復号化鍵の元データとすることができるので、パスワードを変更することにより無数の異なるコード列を生成することができ、異なる無数の暗号化鍵および復号化鍵を生成することが可能となる。

【0072】また、指紋読み取りデータを照合するための照合データを記憶手段に記憶することがないので、第三者による照合データの盗難の恐れがなく、不正に暗号鍵を複製される恐れがない。

【0073】次に、図4を用いて、上述の暗号化装置、復号化装置、および暗号化・復号化装置のハードウェア構成について説明する。

【0074】図4は、図1～3において説明した暗号化装置、復号化装置、および暗号化・復号化装置に関するハードウェア構成の一例を示すブロック図である。

【0075】指紋読み取り手段400は、光学的な指紋パターン読み取り手段としてのスキャナ402、マイクロコンピュータ#1:403を含む。マイクロコンピュータ#1:403は、バス404にCPU405、ROM406、RAM407、インプット・アウトプット・インタフェース(I/O)408を接続した構成を持つ。

【0076】マイクロコンピュータ#1:403を構成するROM406は、マイクロコンピュータ#1:403を起動しオペレーティングシステム(OS)等を立ち上げるための基本プログラム等を格納し、RAM407は、主記憶用メモリとして使用され、CPU405によるコード生成処理等、各種処理のための作業領域を備え

ている。各種プログラム、例えば、指紋コード生成プログラムは図示しないフロッピー(登録商標)ディスクやハードディスク等の記憶媒体に格納され、実行時にRAM407にロードされるようにしてもよい。

【0077】スキャナ402において読み取られた指紋画像データは、I/O408を介してマイクロコンピュータ#1:403に入力され指紋コードを生成する処理が実行される。

【0078】指紋読み取り手段400における処理、すなわちスキャナ402によって読み取られた指紋画像データから指紋コードを生成する処理について図5を用いて説明する。

【0079】なお、本発明の暗号化・復号化装置および暗号化・復号化方法においては、暗号鍵の生成元となるコードは、指紋等の生体情報コードと入力パスワードの双方に基づいて形成される。従って、入力パスワードを変更することによって合成して生成されるコードをいかにでも複雑化することが可能であるので、指紋等の生体情報コード自体は複雑なコードとすることが要請されない。生体情報から得られるコードを単純な短いデータ列としても、パスワードと組み合わせたコード列において同一コードが生成される可能性はほとんどない。従って、指紋読み取り精度を高くすることなく、高度なスキャン装置が必要とされない。

【0080】従来の生体情報のみに頼るコード生成手法では、異なる個人の指紋等から読み取られる生体情報コードが同一になってしまうと、その同一コードに基づいて同一の暗号鍵が生成される可能性がある。このような可能性を排除するため、スキャナの読み取り精度を極めて高精度にして各個人の生体情報コードを確実に異なるものとするのが要請されていた。しかし、現実には、高精度な読み取りを実行させると、同一人であっても読み取り時毎に異なる指紋コードが生成されるなどの不具合も発生し、使用に耐えるシステムは実現されていないのが現状である。

【0081】本発明の暗号化・復号化装置および暗号化・復号化方法においては、上述のような従来システムとは異なり、生体情報のみではなく、任意のパスワードを組み合わせたコードに基づいて暗号鍵を生成する構成であるので、異なる個人において生体情報が万が一、一致した場合であっても、パスワードとの組み合わせで生成されるコードが一致する可能性はまずない。従って、指紋パターン等の生体情報の読み取りによって取得するコードは極めて簡単な構成とすることが可能である。本発明の暗号化・復号化装置において適用可能な指紋パターン読み取りおよびコード生成の一例を図5を用いて説明する。

【0082】指紋パターンからコードを生成するため、まず、図5(a)に示すように、スキャナに指を触れたときに形成される指紋像を複数領域に分割する。指

の中心部を直交する線により、画像を領域1～4の4つの領域に分割し、分割各領域においてコードを生成する。

【0083】図5(b)は、指紋の隆線方向(指紋の線の流れ)を4つのパターンに分類し、それぞれに対するコードを付与したものである。水平方向の隆線を0(00)、右上がりの隆線を1(01)、垂直方向の隆線を2(10)、右下がりの隆線を3(11)としてコードを対応付けている。

【0084】図5(c)は、図5(a)の指紋パターンの各領域における隆線パターン、すなわち各領域の指紋の隆線方向(指紋の線の流れ)を平均化して、図5(b)の各パターン中、最も類似するパターン選択して指紋パターンと選択パターンを併せて示した図である。

【0085】図5(c)の各領域において指紋パターンともっとも類似する選択パターンの持つコードを領域1～4の順に並べて生成されるデータを指紋コードとした。すなわち、図5の例では、図5(d)に示すように11011101(2進数)、あるいはdd(16進数)を指紋パターンに基づくコード、すなわち指紋コードとして出力される。

【0086】なお、図5で示すコード生成例は、生体情報からコードを生成する1つの例にすぎない。図5では領域分割数を4(図5(a)参照)とし、またコードを対応付けたコード対応パターンについても4種類(図5(b)参照)とした例であるが、領域分割数を4以上の8、あるいは16等に増やしてもよく、また、コード対応パターンについても、さらに方向を細かく区切ってコードを増加させることで、各指紋パターンに応じた細かな分類づけ、コード生成処理が可能である。

【0087】図6に図4に示す指紋読み取り手段400における処理である読み取り指紋画像データから指紋コードを生成する処理フローを示す。図6は、具体的には、図4の指紋読み取り手段400におけるマイクロコンピュータ#1:403の指紋コード読み取りの処理アルゴリズムを示すフローチャートである。

【0088】ステップ601は、図4に示すスキャナ402において読み取られた指紋データを2次元のイメージデータへ展開し、方向の修正、ノイズ処理等の前処理を実行するステップである。

【0089】ステップ602は、ステップ601において前処理されたイメージデータを、n個の領域へ分割する処理を実行するステップである。分割された各領域を(I1, I2, ..., In)とする。

【0090】ステップ603は、ステップ602において分割された領域毎に、そのイメージデータの特徴抽出を行い、その特徴量をコード化するステップである。各領域I1, I2, ..., Inから出力されるコード列を、(C1, C2, ..., Cn)とする。

【0091】ステップ604では、各領域から出力され

たコードを合成し、1つのコードへと合成する。その合成方法の一例は、単純に各領域のコードをつなげる、すなわち接続する方法である。合成コードをAとすると、 $A = C1C2 \dots Cn$ として示される。

【0092】ステップ605は、上記のステップ604において求めたコードAを指紋コードとして出力する。

【0093】指紋読み取り手段400は、このような手順を実行することにより、暗号鍵生成のために必要となる指紋コードを生成する。

【0094】このようにして生成された指紋パターンから得られるコードは、図4の暗号鍵生成手段420に出力される。

【0095】暗号鍵生成手段420は、マイクロコンピュータ#2:423を含む。マイクロコンピュータ#2:423は、バス424にCPU425、ROM426、RAM427、インプット・アウトプット・インタフェース(I/O)428を接続した構成を持つ。

【0096】マイクロコンピュータ#2:423を構成するROM426は、マイクロコンピュータ#2:423を起動しオペレーティングシステム(OS)等を立ち上げるための基本プログラム等を格納し、RAM427は、主記憶用メモリとして使用され、CPU425による暗号鍵生成処理等、各種処理のための作業領域を備えている。各種プログラム、例えば、暗号鍵生成プログラムは図示しないフロッピーディスクやハードディスク等の記憶媒体に格納され、実行時にRAM427にロードされるようにしてもよい。

【0097】指紋読み取り手段400において読み取られ、生成されたコードは、I/O428を介してマイクロコンピュータ#2:423に入力され、暗号鍵生成処理が実行される。

【0098】暗号鍵生成手段420は、指紋読み取り手段400において読み取られ、生成されたコードを入力するとともに、パスワード入力手段410から入力されるパスワードを入力する。パスワード入力手段410は、文字入力するためのキーボード411を備え、ユーザは任意のパスワードを入力できる。

【0099】暗号鍵生成手段420は、指紋読み取り手段400において読み取られ生成されたコードと、パスワード入力手段410から入力されるパスワードに基づいて暗号鍵を生成する。

【0100】暗号鍵生成手段420は、例えば図7に示す機能構成を持つ。図7は、図4に示すマイクロコンピュータ#2:423において実行される処理を、暗号鍵生成のアルゴリズムに従って機能構成に分割して示した機能ブロック図である。図7に示すように、暗号鍵生成手段701は、その処理機能として中間コード生成部711、暗号鍵生成部712を有する。

【0101】中間コード生成部711は、指紋読み取り手段から読み取られた指紋コードとパスワード入力手段

から入力されたパスワードの組み合わせに応じて、中間コードを生成し暗号生成部712に出力する。

【0102】暗号鍵生成部712は、中間コード生成部711から出力された中間コードに所定の関数を施すことにより暗号鍵を生成し、暗号化・復号化手段に出力する。暗号鍵生成部712が生成する鍵は、システムが使用している暗号化方式が例えばDES暗号などの共通鍵方式のときは共通鍵であり、またRSA暗号などの公開鍵方式を使用している場合は、秘密鍵、公開鍵となる。

【0103】中間コード生成部711は、前述の図5、図6を用いて説明したような手法で指紋読み取り手段で読み取られた指紋パターンに基づいて生成された指紋コードと、パスワード入力手段から入力されたパスワードを結合して中間コードを生成する。

【0104】中間コード生成部711において実行される中間コードの生成例を図8に示す。指紋読み取り手段において読み取られた指紋コードが、例えば、16ビットで、

FE26(指紋コード)・・・(1)

であり、また、パスワード入力手段から入力されたパスワードが、例えば、16ビットで、
35BA(パスワード)・・・(2)

であったと仮定する。

【0105】中間コード生成部611は、上記(1)の指紋コードと、(2)のパスワードを合成して、

FE2635BA・・・(3)

の32ビットの中間コードを生成する。

【0106】図7に示す中間コード生成部711において生成された中間コードは、暗号鍵生成部712へ出力される。

【0107】なお、図8に示す中間コードの生成例は、1つの例であり、中間コードは指紋読み取り手段において生成される指紋コードと、パスワード入力手段によって入力されるパスワードに基づいて生成されるデータであれば許容されるものであり、図8に示すようなコード連接処理に限らず、指紋コードとパスワードに基づく新たなコードを生成すればよいものである。例えば、指紋コードとパスワードに対して関数を適用して中間コードを得る構成としてもよく、また、指紋コードとパスワードをアドレスとするテーブル検索による処理等によって新たなコードを生成してもよい。

【0108】中間コード生成部711において生成された中間コードは、暗号鍵生成部712に出力され、暗号鍵生成部712は中間コードに基づいて暗号鍵を生成する。暗号鍵の生成手法は、RSA方式、DES方式等、システムの採用している方式に従って処理が行なわれることになる。

【0109】図9に図9(a)として共通鍵暗号化方式の場合の暗号鍵生成処理に用いる機能ブロック構成、図9(b)として公開鍵暗号化方式の場合の暗号鍵生成処

理に用いる機能ブロック構成をそれぞれ示す。

【0110】図9(a)の共通鍵暗号化方式について、まず説明する。先に説明したように共通鍵暗号化方式は、暗号化するとき使用する鍵と、復号化するとき使用する鍵とを共通化した暗号化方式である。

【0111】図9(a)に示す共通鍵暗号化方式における暗号鍵生成部901は、関数Fを適用する関数処理手段902を有し、中間コード生成部から受領する中間コードに関数Fを適用して暗号化鍵、復号化鍵を生成して暗号化・復号化手段に出力する。関数Fの例としては、例えばMD4ハッシュ関数、またはMD5ハッシュ関数等の一方向関数がある。先に説明したように、生成された暗号鍵に基づいて、元のデータ、この場合は中間コードを導くことは困難である。

【0112】共通鍵暗号化方式を採用している場合は、このようにして生成された暗号化鍵、または復号化鍵を用いて、データの暗号化処理または復号化処理が実行されることになる。

【0113】次に図9(b)の公開鍵暗号化方式について説明する。図9(b)を用いてRSA方式を採用している場合の暗号鍵生成処理について説明する。図9

(b)に示すように暗号鍵生成部903は、中間コード分割部904、素数生成器905、公開鍵・秘密鍵生成部906を有する。

【0114】RSA方式において公開鍵と、秘密鍵を生成するためには、2個の素数 p 、 q が必要となる。中間コード分割部904では、中間コード生成部から入力される中間コードを2つのコードに分割する。例えば中間コードを途中で区切り、上位ビットと下位ビットの2つのコードを生成する。

【0115】中間コード分割部904で生成された2つのコードは素数生成器905に出力される。素数生成器805は乱数発生器を有する。中間コード分割部904で生成された2つのコードのそれぞれが素数生成器805の有する乱数発生器に対する種として使用され、乱数発生器で発生された乱数をもとに素数判定し、素数が2つ抽出される。抽出された2つの素数が、暗号鍵生成用の素数 p 、 q として公開鍵・秘密鍵生成部906に対して出力される。

【0116】公開鍵・秘密鍵生成部906は、素数 p 、 q に基づいて公開鍵、秘密鍵を生成する。 p 、 q は、素数生成器905が生体情報コードとパスワードに基づく分割中間コードに基づいて出力した2つの素数 p 、 q であり、十分に大きな素数(例えば512～2048ビット)である。

【0117】公開鍵・秘密鍵生成部906における暗号鍵の生成処理は、例えば以下の手順で行なわれる。まず、 $f = (p-1)(q-1)$ とし、この f に互いに素(最大公約数が1)である値、 e を求める。すなわち $gcd(e, (p-1), (q-1)) = 1$ を満足する

値、 e を求める。なお、 gcd は最大公約数を意味する。さらに、 $ed = 1 \pmod{f}$ とする値、 d を求め、これら各値に基づいて公開鍵を n 、 e とし、秘密鍵を p 、 q 、 d として決定する。

【0118】公開鍵・秘密鍵生成部906の生成した公開鍵、秘密鍵は、素数 p 、 q を知っていれば d をユークリッドの互除法で求めることができるが、 p 、 q を知らないものは、 d を求めるためには n を因数分解することが必要となり、これは膨大な計算量となるため、実質的に値 d を求めることは不可能である。公開鍵・秘密鍵生成部906は、このような手順に従って、公開鍵・秘密鍵を生成する。なお、システムが適用している暗号化方式が異なれば鍵の生成方法も異なってくる。

【0119】図4に戻って、本発明の暗号化・復号化装置の構成について説明を続ける。暗号鍵生成手段420では、上述した手法に従って各種の暗号鍵を生成する。

【0120】暗号鍵生成手段420の生成した暗号鍵は、暗号化・復号化手段430に送られる。図4に示す例では、暗号化・復号化手段430として暗号化処理、復号化処理のいずれでも実行可能な構成、すなわち、図3に対応する暗号化・復号化装置の構成として示してあるが、図1または図2に示すように暗号化処理装置、または復号化処理装置である場合は、暗号化処理、または復号化処理のいずれか一方を実行する構成となる。

【0121】暗号化・復号化手段430は、図4に示すように、マイクロコンピュータ#3:433を含む。マイクロコンピュータ#3:433は、バス434にCPU435、ROM436、RAM437、インプット・アウトプット・インタフェース(I/O)438を接続した構成を持つ。

【0122】マイクロコンピュータ#3:433を構成するROM436は、マイクロコンピュータ#3:433を起動しオペレーティングシステム(OS)等を立ち上げるための基本プログラム等を格納し、RAM437は、主記憶用メモリとして使用され、CPU435による暗号化処理、復号化処理等、各種処理のための作業領域を備えている。各種プログラム、例えば、暗号化処理プログラム、または復号化プログラムは図示しないフロッピーディスクやハードディスク等の記憶媒体に格納され、実行時にRAM437にロードされるようにしてもよい。

【0123】暗号鍵生成手段420において生成された暗号鍵は、I/O438を介してマイクロコンピュータ#3:433に入力され、暗号化処理、または復号化処理が実行される。

【0124】暗号化・復号化手段430は、データ入力手段440から暗号化の対象となるデータ、または復号対象となる暗号化データを入力する。データ入力手段440は、図4の例では、記憶装置としてのハードディスク441を備え、ハードディスク中に処理対象のデータ

が格納されたものを想定しているが、データ入力は、例えばネットワークを介して転送されてくるデータであってもよい。

【0125】暗号化・復号化手段430において、暗号化処理、または復号化が実行されたデータは、データ出力手段450に出力される。図4ではデータ出力手段450としてネットワークインタフェース451を記載しているが、このようにネットワークインタフェース451を介して外部に出力する構成、あるいはハードディスク、光ディスク、その他の記憶媒体に処理データを格納する構成としてもよい。

【0126】暗号化・復号化手段430において実行される暗号化処理、または復号化処理は、前述の共通鍵暗号化方式、公開鍵暗号化方式等に基づいて、例えばRSA方式、DES方式等が適用されて処理が実行され、暗号化情報の生成、または暗号データからの復号データの生成が実行される。

【0127】以上の説明から明らかなように、本発明の暗号化・復号化装置および暗号化・復号化方法においては、共通鍵暗号化方式、公開鍵暗号化方式いずれの暗号化方式においても、指紋読み取り手段400による指紋情報から生成される個人特有の生体情報コードと、パスワード入力手段410から入力されるパスワードとに基づいて暗号鍵生成手段420において暗号鍵が生成され、この暗号鍵に基づいてデータの暗号化処理、または復号化が実行されることになるので、個人固有の鍵生成が可能となり、また、様々なパスワードを組み合わせることで多様な鍵を無数に生成することが可能となる。

【0128】さらに、本発明の構成によれば、暗号鍵の生成元データの一部を構成するパスワードを例えばハードディスク等の記憶装置に記憶し、暗号化処理、復号処理を行なう場合にのみ生体情報と合成して中間コードを生成して暗号鍵を生成する構成としてもよい。パスワードのみからは同じ暗号鍵を生成することができないので、記憶装置からパスワードが盗まれてもデータの復号処理には適用できない。従って、複雑なパスワードを使用したい場合は、これを記憶媒体に記憶して管理することができ機密管理が容易となる。

【0129】なお、図4に示すハードウェア構成例では指紋読み取り手段400、暗号鍵生成手段420、暗号化・復号化手段430をそれぞれ個別のマイクロコンピュータとして示してあるが、指紋読み取り、暗号鍵生成、暗号化・復号化処理は、1つのコンピュータによって順次処理することも可能であり、図4に示すように複数のコンピュータによる構成のみならず、様々な構成が可能である。

【0130】また、上述の実施例では、生体情報として指紋情報を用いた例を説明したが、先にも述べたように、指紋以外にも、「その人固有の情報」、たとえば、声紋や、眼底パターン、DNAパターンなどに基づい

て、生体コードを生成し、このコードとパスワードとを組み合わせた合成コードに基づいて暗号化、復号化する構成としてもよい。さらに、生体コード自体を指紋コードと声紋コードとの合成コード、指紋コードと眼底パターンとの合成コードとし、これらにさらにパスワードを組み合わせる暗号鍵生成用のコードとしてもよい。

【0131】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0132】

【発明の効果】以上、説明したように、本発明の暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法によれば、指紋コードのような各種の生体情報とパスワードとを組み合わせた合成コードを生成し、この合成コードに基づいて暗号鍵を生成する構成とした。従って、パスワードによる合成コードのユニーク性を高め、固有のものとするのが可能となり、異なる個人間において読み取り生体情報が万が一、一致した場合であっても、パスワードとの組み合わせで生成されるコードは異なるものとするのが可能であるので、指紋パターン等の生体情報の読み取りによって取得するコードを極めて簡単なコードとすることが可能となり、高精度の読み取り装置を必要としない暗号化・復号化装置構成が実現される。

【0133】さらに本発明の暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法においては、記憶装置等に予め正規ユーザの生体情報を登録して照合処理を実行する構成ではないので、利用可能な装置が照合データを持つシステムに限られず、拡張性の高い構成が実現される。

【0134】さらに、本発明の暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法においては、生体情報にパスワードを組み合わせたコード列に基づいて暗号化鍵、または復号化鍵を生成する構成としたので、パスワードを変更することにより無限数の異なる暗号化鍵または復号化鍵の生成が可能となる。

【0135】さらに、本発明の暗号鍵生成装置、暗号化・復号化装置および暗号鍵生成方法、暗号化・復号化方法においては、パスワードのみからは同じ暗号鍵を生成することができないので、記憶装置にパスワードを記憶して管理することができ機密管理が容易となる。

【図面の簡単な説明】

【図1】本発明に係る暗号化装置の構成を示すブロック図である。

【図2】本発明に係る復号化装置の構成を示すブロック

図である。

【図3】本発明に係る暗号化・復号化装置の構成を示すブロック図である。

【図4】本発明に係る暗号化装置、復号化装置、暗号化・復号化装置のハードウェア構成を示すブロック図である。

【図5】本発明の暗号化・復号化装置における指紋パターンからコードを生成する処理例を説明する図である。

【図6】本発明の暗号化・復号化装置における指紋パターンからコードを生成する処理フローを示す図である。

【図7】本発明の暗号化・復号化装置における暗号鍵生成手段の処理ブロック図を示す図である。

【図8】本発明の暗号化・復号化装置における暗号鍵生成手段の指紋コード、パスワード、および中間コードの例を示す図である。

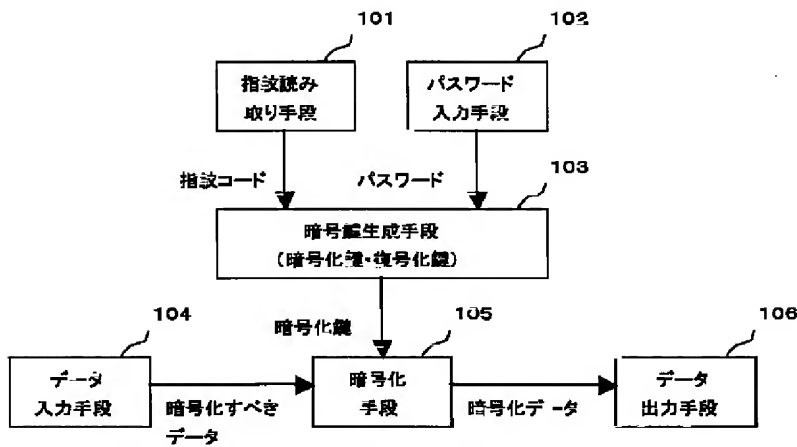
【図9】本発明の暗号化・復号化装置における暗号鍵生成手段の共通鍵暗号化方式と公開鍵暗号化方式における構成を示すブロック図である。

【符号の説明】

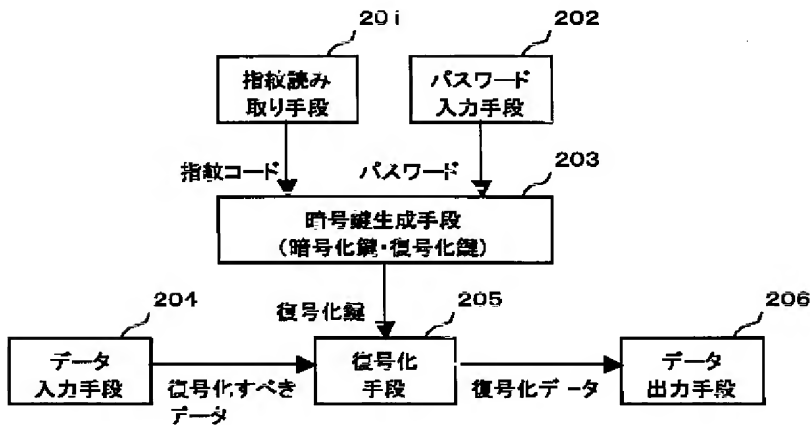
- 101, 201, 301 指紋読み取り手段
- 102, 202, 302 パスワード入力手段
- 103, 203, 303 暗号鍵生成手段
- 104, 204, 304 データ入力手段
- 105 暗号化手段
- 106, 206, 306 出力手段
- 205 復号化手段
- 305 暗号化・復号化手段
- 400 指紋読み取り手段
- 402 スキャナ
- 403, 423, 433 マイクロコンピュータ
- 404, 424, 434 バス
- 405, 425, 435 CPU
- 406, 426, 436 ROM
- 407, 427, 437 RAM
- 410 パスワード入力手段
- 411 キーボード
- 420 暗号鍵生成手段
- 430 暗号化(復号化)手段
- 440 データ入力手段
- 441 ハードディスク
- 450 データ出力手段
- 451 ネットワークインタフェース
- 701 暗号鍵生成手段
- 711 中間コード生成部
- 712 暗号鍵生成部
- 901 暗号鍵生成手段
- 902 関数処理手段
- 903 暗号鍵生成手段
- 904 中間コード分割部
- 905 素数生成器

906 公開鍵・秘密鍵生成部

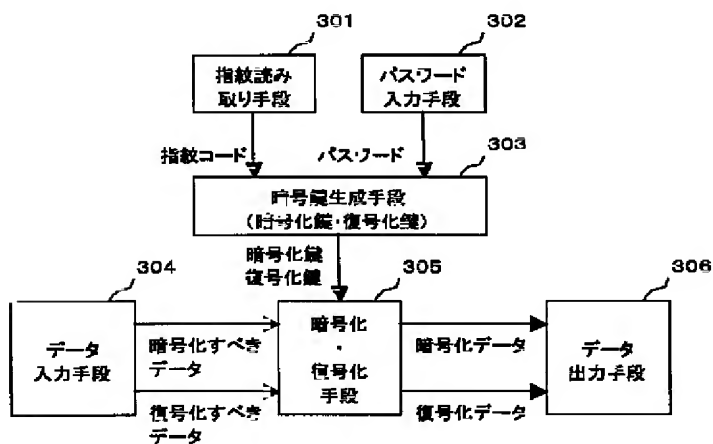
【図1】



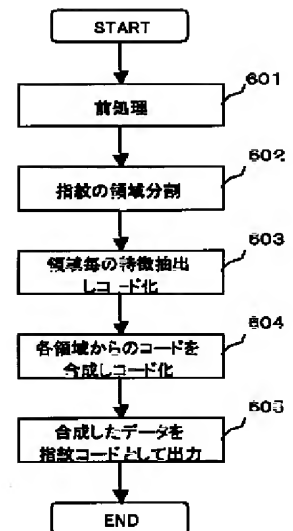
【図2】



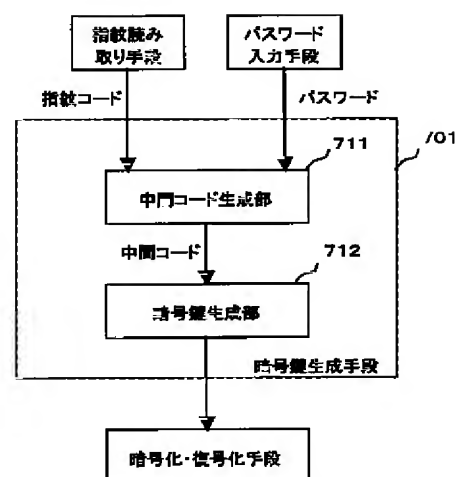
【図3】



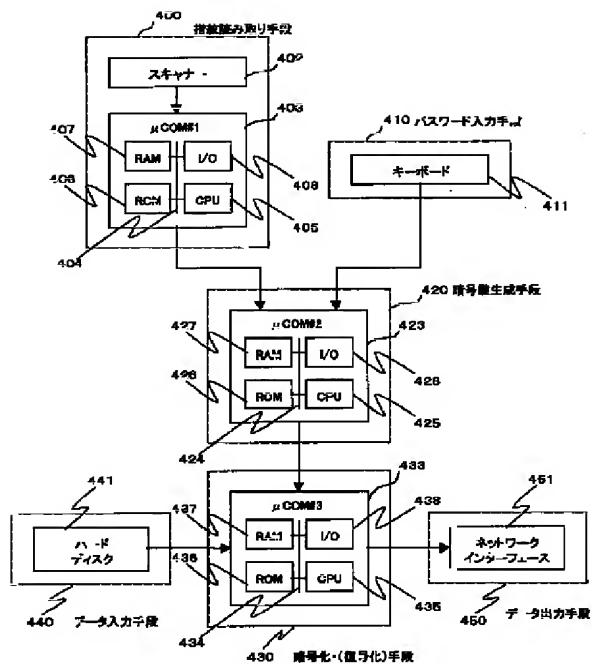
【図6】



【図7】



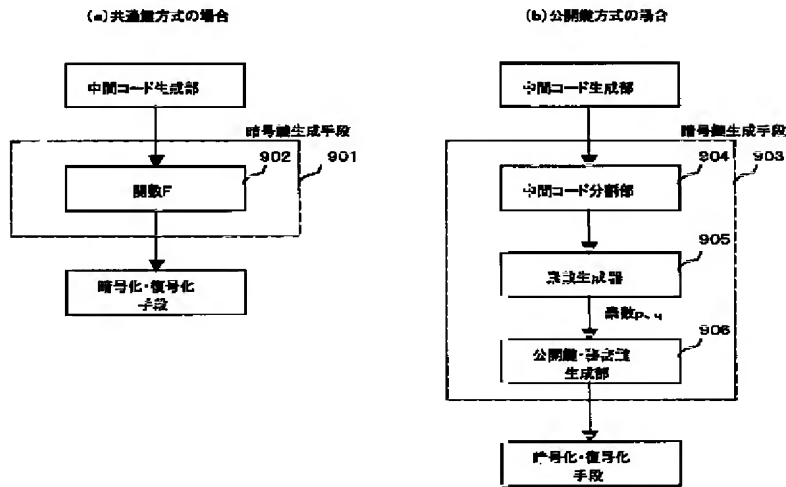
【 図 4 】



【 図 8 】

指紋コード	パスワード	中間コード
FE26	35BE	FE2635BE

【 図 9 】



【 図 5 】

